"That One's Gotta Work"

How Mars Odyssey used a Fault Tree Driven Risk Assessment Process to Reduce Risk

The Odyssey project was the first mission to be launched to Mars since the failures of the two Mars Surveyor Program '98 spacecraft, the Mars Climate Orbiter (MCO) and the Mars Polar Lander. Due to those failures, a much larger emphasis on risk identification and reduction became apparent. In addition to incorporating the results of the Mars '98 failure review boards and responding to external red team reviews, the Odyssey project itself implemented a risk assessment and reduction process using a team of Jet Propulsion Laboratory and Lockheed Martin project personnel led by the author of this paper. At the heart of the process was the use of fault trees, which were used to break the mission down into the functional elements needed to make it a success. By determining how each function could be prevented from executing, a list of failure modes was created. Each failure mode was then individually assessed as to what mitigations (e.g. redundancy, worst case analysis) were in place to ensure the fault does not occur. Each mitigation entry was then tied to a specific test or analysis in the project verification program to ensure that it was explicitly verified.

The first section of the paper will give an overview of the Mars Odyssey project including a description of the project success criteria, mission and spacecraft overviews, and a history of the development. The history description will emphasize the shift in paradigms from a project that was intended to be a build-to-print of the MCO spacecraft with emphasis on cost containment to a project where risk avoidance was the top priority and each item inherited from MCO needed to be re-reviewed in light of that mission's failure.

The second section will describe the risk assessment process itself. It will start with the formation of a risk assessment team comprised of members from across the project to ensure that we would maintain a broad focus. We did not want to limit the risks assessment to spacecraft design issues, but to include everything that could possibly prevent mission success, for example navigation and mission operations. This section will then cover how the mission was broken down into critical phases, how the design and verification was reviewed, and how peer reviews were used to ensure nothing was missed, as well as to transmit risk findings to project management so that they could either accept the risks, or implement steps to reduce or eliminate them.

The third section will describe the fault trees themselves; how they were generated, and what tools were used in their creation. It will touch on issues such as what types of faults were covered and how "deep" the trees were taken. This section will also show how the faults were tied to tables listing risk evaluation categories and mitigation descriptions.

The last section will detail how this risk assessment process was actually used on the Mars Odyssey project. It will detail what risk areas were found, and what the project did with that information.